Dynamic Rule Sets for Generated Logs

Field of the Invention

This invention relates in general to network diagnostics, and more particularly to a network administration system for automatically activating dynamic rule sets in response to satisfying the criteria of existing static rule sets of error logs in a network.

Background of the Invention

It is well known in traditional computer and digital communication networks for technicians to respond to the generation of error logs by notifying affected users of system problems, analyzing and then fixing the problems using an assortment of software commands and/or tools. The use of such software commands is often repetitive and requires the technician to manually enter the commands upon each observation of a specific log. Thousands of logs can be generated by a single problem. For example, if a T1 line goes down, error logs could be generated by thousands of phones that cannot find a dial tone.

Therefore, according to the prior art, automatic filtering of error logs has been effected through the use of "rule sets" to determine if a combination of logs satisfies a given criteria. One example of such an automated process is a product from Plexis (http://www.triadhc.com/edi.shtml) called Plexis EDI Toolkit. If the criteria is satisfied, it is known in the art either to generate a further log or to provide an overall summary for describing the problem to the technician. Thus, it is known to generate Higher Level Logs (HLL) from Lower Level Logs (LLL) in response to predetermined rule sets being satisfied. The Lower Level Logs (LLL) are generated by network applications or devices. Such systems are valuable because the HLLs help to explain to the system administrator/designer what is really going on in the system.

There are instances where HLL's generate more HLL logs, or combinations of LLL's and HLL's generate new HLL's. According to the prior art, these rule sets are either manually applied by the technician as required, which can be a time consuming and complicated task where many logs have been generated, or the rule sets remain

activated at all times, in which case analysis of the logs becomes time consuming since many rule sets need to be examined.

Summary of the Invention

According to the present invention, a network administration system is provided for automatically activating and deactivating dynamic rule sets when specified static rule sets have been satisfied. The static rule sets whose criteria have been satisfied by the generation of predetermined error logs trigger activation or deactivation of the dynamic rule sets. The automatic activation and deactivation of dynamic rule sets alleviates time consuming manual application of rule sets. The causal activation and deactivation of the dynamic rule sets only when other rule set criteria have been satisfied reduces the number of rule sets when compared to the prior art approach of activating all rule sets at all times.

The system of the present invention may advantageously be applied to any application that generates logs and is monitored by rule sets, to allow dynamic variations in monitoring when different problems arise, and to set explicit instructions for specific circumstances of logs.

Brief Description of the Drawings

A detailed description of the preferred embodiment is set forth herein below with reference to the following drawings, in which:

Figure 1 is a block diagram of an exemplary network incorporating the system of the present invention;

Figure 2 is a table of a set of rules that have been defined for use in the network of Figure 1;

Figure 3 is a table showing an exemplary list of logs generated by the network of Figure 1;

Figure 4 shows a graphical user interface for entering dynamic rule sets; and

Figure 5 is a flowchart showing activation and deactivation of dynamic rule sets.

Detailed Description of the Preferred Embodiment

Figure 1 shows a typical network comprising a plurality of phones (P1 to P3) connected to a server implemented PBX (PBX 1), a further phone P1 connected to a client server C1, both the client C1 and PBX 1 being connected to a PBX2. The PBX 2 is connected to a T1 trunk in a well known manner. Each of the devices shown in Figure 1, with the exception of the trunk, has the capability of generating logs to inform a technician of the device status. The network configuration is for illustration purposes only, and may incorporate a host of other devices and networks.

As indicated above, Figure 2 demonstrates a set of rule sets that are defined for use in the network in Figure 1, and Figure 3 shows a typical list of logs (HLL's and LLL's) that are generated from the network in Figure 1 as well as associated explanations of how dynamic rule sets are created. The explanation does not form part of the error log, which is restricted to the Log ID, Time Generated and Brief Description. The system parses the Brief Description in order to identify the source of a particular error log.

According to the invention, a network administration system is provided for programming the activation and deactivation of dynamic rule sets in response to network conditions. Thus, with reference to Figure 4, a user interface is provided for activating and deactivating certain rule sets (identified by rule set Ids, such as RSID001, RSID02, etc), and associating rule set activation and deactivation keys. Thus, the rule set identified by RSID001 has been activated by the user and programmed to activate rules sets RSID004 and RS005 when its rule set criteria have been satisfied (i.e. LogP6000 or LogP6001 or LogP6002) have been received from two or more phones). When the criteria for rule set RSID001 have been satisfied, HLL001 will be generated and the Rule Set Status for RSID004 and RSID005 will

change in Figure 2 from OFF to ON. Likewise, when the rule set criteria for RSID004 has been satisfied (i.e. more than one hundred system error logs have been counted), HL004 is generated. The activated rule sets remain active until reset by the user, by another rule set, or by timing out. According to the scenario of Figures 2 – 4, RSID006 has been deactivated by the user. However, if activated by the user this rule set monitors the faulty T1 trunk for activity (i.e. the rule set is Search for > 2 ping T1 logs). The log details of Figure 3 shown LOGT001 being generated three times in succession, thereby satisfying the RSID006 rule set which, according to the user configuration of Figures 2 and 4, results in self-deactivation of the rule set (as well as deactivation of rule set RSID007).

The activation and deactivation of rule sets is triggered by using software tools (e.g. Visual Basic, C++) to read and compare the logs to active rule sets, as shown in Figure 5. If a rule set is fully satisfied, its rule set ID is compared with the rule set Ids of any associated activation keys (as programmed by the user). If the rule set has activation keys programmed, the first such activation key is read, the status of the specified rule set is changed, and remaining activation keys are read and changed in the same manner until no activation keys remain for the rule set.

Exemplary pseudo-code of the process for implementing the network administration system of the present invention is as follows:

```
Dynamic rule sets function prog
        Retrieve log
        Compare logs with rule sets
        If rule set fully satisfied
                If rule set has activation keys
                        Go to first activation key
                        While activation keys exist
                                Set status of specified rule set id
                                Go to next activation key
                        endwhile
                endif
        endif

End dynamic rule sets function prog
```

Alternatives and modifications of the invention are possible within the sphere and scope as set forth in the claims appended hereto.